F? By Theorem 5.3.2, $[E:F] \leq 3! = 6$; by the above remark, since $x^3 - 2$ is irreducible over F and since $[F(\sqrt[3]{2}):F] = 3$, by the corollary to Theorem 5.1.1, $3 = [F(\sqrt[3]{2}):F] \mid [E:F]$. Finally, $[E:F] > [F(\sqrt[3]{2}):F] = 3$. The only way out is $[E:F] = 6$. We could, of course, get this result by making two extensions $F_1 = F(\sqrt[3]{2})$ and $E = F_1(\omega)$ and showing that ω satisfies an irreducible quadratic equation over F_1.

3. Let F be the field of rational numbers and let

$$f(x) = x^4 + x^2 + 1 \in F[x].$$

We claim that $E = F(\omega)$, where $\omega = (-1 + \sqrt{3}\, i)/2$, is a splitting field of $f(x)$. Thus $[E:F] = 2$, far short of the maximum possible $4! = 24$.

Problems

1. In the proof of Lemma 5.3.1, prove that the degree of $q(x)$ is one less than that of $p(x)$.
2. In the proof of Theorem 5.3.1, prove in all detail that the elements $1 + V, x + V, \ldots, x^{n-1} + V$ form a basis of E over F.
3. Prove Lemma 5.3.3 in all detail.
4. Show that τ^{**} in Lemma 5.3.4 is well defined and is an isomorphism of $F[x]/(f(x))$ onto $F[t]/(f'(t))$.
5. In Example 3 at the end of this section prove that $F(\omega)$ is the splitting field of $x^4 + x^2 + 1$.
6. Let F be the field of rational numbers. Determine the degrees of the splitting fields of the following polynomials over F.
   (a) $x^4 + 1$. (b) $x^6 + 1$.
   (c) $x^4 - 2$. (d) $x^5 - 1$.
   (e) $x^6 + x^3 + 1$.
7. If p is a prime number, prove that the splitting field over F, the field of rational numbers, of the polynomial $x^p - 1$ is of degree $p - 1$.

**8. If $n > 1$, prove that the splitting field of $x^n - 1$ over the field of rational numbers is of degree $\Phi(n)$ where Φ is the Euler Φ-function.
(This is a well-known theorem. I know of no easy solution, so don't be disappointed if you fail to get it. If you get an easy proof, I would like to see it. This problem occurs in an equivalent form as Problem 15, Section 5.6.)

*9. If F is the field of rational numbers, find necessary and sufficient conditions on a and b so that the splitting field of $x^3 + ax + b$ has degree exactly 3 over F.

10. Let p be a prime number and let $F = J_p$, the field of integers mod p.
   (a) Prove that there is an irreducible polynomial of degree 2 over F.

(b) Use this polynomial to construct a field with p^2 elements.

*(c) Prove that any two irreducible polynomials of degree 2 over F lead to isomorphic fields with p^2 elements.

11. If E is an extension of F and if $f(x) \in F[x]$ and if ϕ is an automorphism of E leaving every element of F fixed, prove that ϕ must take a root of $f(x)$ lying in E into a root of $f(x)$ in E.

12. Prove that $F(\sqrt[3]{2})$, where F is the field of rational numbers, has no automorphisms other than the identity automorphism.

13. Using the result of Problem 11, prove that if the complex number α is a root of the polynomial $p(x)$ having *real* coefficients then $\bar{\alpha}$, the complex conjugate of α, is also a root of $p(x)$.

14. Using the result of Problem 11, prove that if m is an integer which is not a perfect square and if $\alpha + \beta\sqrt{m}$ (α, β rational) is the root of a polynomial $p(x)$ having *rational coefficients*, then $\alpha - \beta\sqrt{m}$ is also a root of $p(x)$.

*15. If F is the field of real numbers, prove that if ϕ is an automorphism of F, then ϕ leaves every element of F fixed.

16 (a) Find *all* real quaternions $t = a_0 + a_1 i + a_2 j + a_3 k$ satisfying $t^2 = -1$

*(b) For a t as in part (a) prove we can find a real quaternion s such that $sts^{-1} = i$.

5.4 Construction with Straightedge and Compass

We pause in our general development to examine some implications of the results obtained so far in some familiar, geometric situations.

A real number α is said to be a *constructible number* if by the use of straightedge and compass alone we can construct a line segment of length α. We assume that we are given some fundamental unit length. Recall that from high-school geometry we can construct with a straightedge and compass a line perpendicular to and a line parallel to a given line through a given point. From this it is an easy exercise (see Problem 1) to prove that if α and β are constructible numbers then so are $\alpha \pm \beta$, $\alpha\beta$, and when $\beta \neq 0$, α/β. Therefore, the set of constructible numbers form a subfield, W, of the field of real numbers.

In particular, since $1 \in W$, W must contain F_0, the field of rational numbers. We wish to study the relation of W to the rational field.

Since we shall have many occasions to use the phrase "construct by straightedge and compass" (and variants thereof) *the words construct, constructible, construction, will always mean by straightedge and compass.*

If $w \in W$, we can reach w from the rational field by a *finite* number of constructions.

of K. But then they have a nontrivial greatest common divisor over K, which must be a divisor of $x - b$. Since the degree of $x - b$ is 1, we see that the greatest common divisor of $g(x)$ and $h(x)$ in $K[x]$ is exactly $x - b$. Thus $x - b \in K[x]$, whence $b \in K$; remembering that $K = F(c)$, we obtain that $b \in F(c)$. Since $a = c - \gamma b$, and since $b, c \in F(c)$, $\gamma \in F \subset F(c)$, we get that $a \in F(c)$, whence $F(a, b) \subset F(c)$. The two opposite containing relations combine to yield $F(a, b) = F(c)$.

A simple induction argument extends the result from 2 elements to any finite number, that is, if $\alpha_1, \ldots, \alpha_n$ are algebraic over F, then there is an element $c \in F(\alpha_1, \ldots, \alpha_n)$ such that $F(c) = F(\alpha_1, \ldots, \alpha_n)$. Thus the

COROLLARY *Any finite extension of a field of characteristic 0 is a simple extension.*

Problems

1. If F is of characteristic 0 and $f(x) \in F[x]$ is such that $f'(x) = 0$, prove that $f(x) = \alpha \in F$.
2. If F is of characteristic $p \neq 0$ and if $f(x) \in F[x]$ is such that $f'(x) = 0$, prove that $f(x) = g(x^p)$ for some polynomial $g(x) \in F[x]$.
3. Prove that $(f(x) + g(x))' = f'(x) + g'(x)$ and that $(\alpha f(x))' = \alpha f'(x)$ for $f(x), g(x) \in F[x]$ and $\alpha \in F$.
4. Prove that there is no rational function in $F(x)$ such that its square is x.
5. Complete the induction needed to establish the corollary to Theorem 5.5.1.

An element a in an extension K of F is called *separable over* F if it satisfies a polynomial over F having no multiple roots. An extension K of F is called *separable* over F if all its elements are separable over F. A field F is called *perfect* if all finite extensions of F are separable.

6. Show that any field of characteristic 0 is perfect.
7. (a) If F is of characteristic $p \neq 0$ show that for $a, b \in F$, $(a + b)^{p^m} = a^{p^m} + b^{p^m}$.
   (b) If F is of characteristic $p \neq 0$ and if K is an extension of F let $T = \{a \in K \mid a^{p^n} \in F \text{ for some } n\}$. Prove that T is a subfield of K.
8. If K, T, F are as in Problem 7(b) show that any automorphism of K leaving every element of F fixed also leaves every element of T fixed.

*9. Show that a field F of characteristic $p \neq 0$ is perfect if and only if for every $a \in F$ we can find a $b \in F$ such that $b^p = a$.

10. Using the result of Problem 9, prove that any finite field is perfect.